



System and Organization Controls Report

SOC 3 Report

Relevant to Security, Availability, and Confidentiality

June 1, 2024 – May 31, 2025

Deloitte.

Section I:

Independent Service Auditor Report

Independent Service Auditor's Report

To: Management of RavenDB Ltd.

Ahad Ha'Am St. 9, Hadera, Israel

Scope

We have examined RavenDB Ltd.'s (the "Service Organization" or "RavenDB") accompanying assertion titled "Assertion of RavenDB Ltd. Management" (assertion) that the controls related to RavenDB platform were effective throughout the period June 1, 2024 to May 31, 2025 (the "Description"), to provide reasonable assurance that RavenDB Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria").

The description of the boundaries of the system indicates that certain applicable trust services criteria specified in the description of the boundaries of the system can be met only if complementary user-entity controls contemplated in the design of RavenDB's controls are suitably designed and operating effectively, along with related controls at RavenDB. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

RavenDB uses Amazon Web Services (AWS) for its cloud computing services ("subservice organization"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RavenDB, to achieve RavenDB's service commitments and system requirements based on the applicable trust services criteria. The Description presents RavenDB's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of RavenDB's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

RavenDB Ltd. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that RavenDB's service commitments and system requirements were achieved. RavenDB has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, RavenDB is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities



Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

Obtaining an understanding of the system and the service organization's service commitments and system requirements.

Assessing the risks that controls were not effective to achieve RavenDB's service commitments and system requirements based on the applicable trust services criteria.

Performing procedures to obtain evidence about whether controls within the system were effective to achieve RavenDB's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.



Opinion

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RavenDB Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

August 27, 2025

A handwritten signature in blue ink, reading "Brightman Almagor Zohar & Co.".

Brightman Almagor Zohar & Co.

Certified accountants

A firm in the Deloitte Global Network

Section II:

Management of RavenDB's Assertion



Assertion of RavenDB's Management

Assertion of RavenDB Ltd.

We are responsible for designing, implementing, operating, and maintaining effective controls within RavenDB Ltd. Service Organization's (RavenDB's) system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RavenDB's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

RavenDB uses Amazon Web Services (AWS) to provide Cloud computing service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RavenDB, to achieve RavenDB's service commitments and system requirements based on the applicable trust services criteria. The description presents RavenDB's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of RavenDB's controls. The description does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RavenDB Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria. RavenDB Ltd.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RavenDB Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A



Attachment A

RavenDB Ltd.'s Description of the Boundaries of its System

RavenDB Ltd Business Overview

RavenDB Ltd. is a company that specializes in providing database solutions, particularly through its flagship product, RavenDB, a NoSQL document database. The company's structure and services can be broken down as follows:

Company Structure:

Executive Leadership:

- **CEO and Founder:** The company is led by the CEO, the founder and visionary behind the product. For RavenDB, Oren Eini, also known as Ayende Rahien, is the founder and serves as the primary leader.
- **Executive Team:** This includes other key executives who handle operations, marketing, sales, and finance.

Product Development:

- **Engineering and Development Teams:** These teams focus on the core development of the RavenDB database, ensuring it is scalable, reliable, and innovative. They handle product updates, new features, bug fixes, and overall maintenance.
- **Quality Assurance (QA):** A dedicated team ensures the product is thoroughly tested before release, maintaining high standards of performance and reliability.

Sales and Marketing:

- **Sales Team:** Focuses on client acquisition, customer relationship management, and expanding market reach. They engage with enterprises, small to medium-sized businesses, and developers.
- **Marketing Team:** Handles branding, content creation, digital marketing, and community engagement to promote RavenDB and its features.

Customer Support and Success:

- **Technical Support:** A team dedicated to helping clients troubleshoot issues, optimize their databases, and ensure smooth operation.
- **Customer Success:** Focuses on ensuring customers get the most out of RavenDB, helping them with deployment strategies, and offering advice on best practices.

Consulting and Professional Services:

- **Consultants and Trainers:** Experts who provide consulting services to help businesses with implementation, scaling, and optimizing their use of RavenDB.
- **Training Services:** Offers workshops, webinars, and on-site training to educate users on how to effectively use the database.



Services Provided:

1. RavenDB NoSQL Database:

- **On-Premise and Cloud Deployment:** RavenDB can be deployed on-premises or in the cloud, giving businesses flexibility depending on their infrastructure needs.
- **High Availability and Replication:** The database offers features such as clustering, replication, and failover support, ensuring data is always available and resilient to failures.
- **Multi-Model Capabilities:** RavenDB is primarily a document database but also supports graph and time-series data, making it versatile for various use cases.
- **Full-Text Search:** Built-in search capabilities using Lucene.NET, allowing for powerful and efficient data retrieval.
- **ACID Transactions:** RavenDB offers full ACID (Atomicity, Consistency, Isolation, Durability) compliance for transactions, even in a distributed environment.

2. RavenDB Cloud:

- A fully managed database-as-a-service (DBaaS) offering where RavenDB handles all the infrastructure, maintenance, and scaling, allowing businesses to focus on their applications.
- **Multi-Cloud Support:** RavenDB Cloud can run on major cloud platforms such as AWS, Azure, and Google Cloud.

3. Consulting Services:

- **Performance Tuning:** Experts help optimize the performance of existing RavenDB deployments.
- **Architecture Review:** Consulting on how to structure data, choose the right deployment strategy, and use the database effectively.
- **Custom Development:** Tailored solutions and integrations to meet specific business needs.

4. Training and Workshops:

- **Developer Training:** Workshops and courses to teach developers how to best utilize RavenDB's features.
- **Webinars and Online Resources:** Regular webinars and an extensive knowledge base to help users stay updated on best practices and new features.

5. Support Plans:

- **Standard and Premium Support:** Different tiers of support plans offering varying levels of service, from basic support to 24/7 coverage and faster response times.

6. Licensing and Subscriptions:

- Flexible licensing options depending on the deployment model (on-premises, cloud) and the scale of the operation.



Principle Service Commitments and System Requirements

The Service Organization's security commitments in regard to the systems and operations are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided to user entities. Those objectives are based on the service commitments that RavenDB Ltd. makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that RavenDB Ltd. has established for the services.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the RavenDB system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- Combat cyber threats by proactively monitoring and protecting RavenDB Ltd. and our customer's data
- Use strong identity management processes to secure data and systems from intrusion.
- Manage infiltration, intrusions, insider threats and anomalies by understanding who is on our networks, why they are on our networks, and what data they have permission to access.

RavenDB establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in RavenDB's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of relevant service provided to its customers.

Organizational Structure

RavenDB's Ltd. Organizational structure contains several teams and roles that impact the services provided as described above. Below listed the main roles and responsibilities impact the services in the scope of this report.

Roles and Responsibilities

The company has formally established requirements that describe the key roles including responsibilities and related job descriptions as required by RavenDB officers. With respect to relevant trust principle areas, there is assignment of responsibility and authority for decision-making in the company.

Chiefs:

Chief Executive Officer (CEO)

- **Description:** The CEO is the highest-ranking executive responsible for the overall management and strategic direction of the company, ensuring that the company achieves its goals and objectives.

Chief Revenue Officer (CRO)

- **Description:** The CRO is responsible for all aspects of revenue generation, including sales, marketing, and customer success, ensuring the company meets its financial objectives.

Chief Technology Officer (CTO)

- **Description:** The CTO is responsible for the company's technological direction, overseeing R&D, IT infrastructure, and ensuring technology initiatives align with business goals.

Other Roles:

Brand Manager, Team Leader

- **Description:** The Brand Manager, Team Leader is in charge of developing and maintaining the company's brand strategy, leading a team to ensure consistent brand messaging across all platforms.

Cloud Team Leader, CISO (Chief Information Security Officer)

- **Description:** The CISO is responsible for managing the cloud infrastructure team and overseeing the company's information security strategy, ensuring secure, scalable, and reliable cloud services.

Head of Developer Relations

- **Description:** The Head of Developer Relations leads the team that builds and maintains relationships with the developer community, ensuring that the company's products meet developers' needs and fostering a supportive developer ecosystem.

Project Manager

- **Description:** The Project Manager oversees the planning, execution, and completion of projects, managing teams, resources, and timelines to ensure successful project delivery.

R&D and Frontend Team Leader

- **Description:** The R&D and Frontend Team Leader is responsible for leading the development of new technologies with a focus on frontend development, ensuring that the user-facing components are effective and efficient.

R&D and QA Team Leader

- **Description:** The R&D and QA Team Leader is responsible for managing both research and development and quality assurance processes, ensuring that new products meet high standards of quality and functionality.

R&D and Support Team Leader

- **Description:** The R&D and Support Team Leader is responsible for managing the development and continuous improvement of products while also overseeing the support team that provides technical assistance to customers.

R&D Team Leader

- **Description:** The R&D Team Leader is responsible for overseeing the development of new products and technologies, driving innovation and ensuring alignment with the company's strategic goals.

Sales Operations Team Leader

- **Description:** The Sales Operations Team Leader oversees the sales operations team, focusing on improving sales processes, managing CRM systems, and supporting the sales team to enhance overall sales performance.

Technical Writer Team Leader

- **Description:** The Technical Writer Team Leader manages a team of technical writers, ensuring the creation of clear, accurate, and user-friendly documentation for the company's products.

UX/UI Team Leader

- **Description:** The UX/UI Team Leader guides the design team in creating user-friendly and visually appealing interfaces, ensuring a seamless user experience across all digital products.

CC1.0 Control Environment Area

The control environment at RavenDB Ltd. is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. It reflects the overall attitude, actions of management and others concerning the importance of controls and the emphasis given to controls in RavenDB's policies, procedures, methods and organizational structure.

The Key elements of RavenDB's control environment includes Oversight by RavenDB's Management Team, HR Policies and practices and integrity and ethical values.

Organization and Management

The RavenDB Management Team meets on a weekly basis and is responsible for following aspects:

Strategic Oversight and Implementation: Team sets the strategic direction and is responsible for implementing these strategies and ensuring they are executed effectively.

Governance and Compliance: Team ensures that the company adheres to legal and regulatory requirements, as well as maintaining high standards of corporate governance.

Operational Management: Overseeing the daily operations of the company, including managing resources, processes, and workflows to ensure efficiency and productivity.



Financial Oversight and Management: Managing the company's finances, including budgeting, financial planning, and monitoring financial performance to ensure the company's financial health.

Human Resources: Hiring, training, and managing employees. This includes developing policies and procedures, resolving conflicts, and ensuring a positive work environment.

Technology Management: Ensuring that the necessary technologies are in place to support business operations and staying competitive with technological advancements.

Risk Management: Identifying potential risks and developing strategies to mitigate them.

Performance Monitoring: Regularly reviewing the company's performance against its goals and making adjustments as needed to stay on track.

CC2.0 Communication and Information

Information security policy and the company standards

An Information Security Policy is in place addressing system requirements for all users. The policy is reviewed and updated on an annual basis and as needed by the Chief Information Security Officer (CISO).

Associates have access to security policies. RavenDB published its IT security policies on its internal drive.

CC3.0 Risk Assessment

Risk Assessment

The Internal Audit function conducts a yearly risk assessment. The risk assessment is used to drive the activities of the internal audit function.

RavenDB Management Team holds periodic meetings among executive management, IT personnel, and legal counsel to identify issues that may affect relevant trust principles.

The functions in the company that are in charge of governance hold periodic reviews of the entity's compensation and performance evaluation programs to identify potential incentives and pressures for employees to commit fraud.

CC4.0 Monitoring Activities

Monitoring

RavenDB has deployed firewalls and rule configurations to protect RavenDB servers against outsiders and threats to the system's security. Firewall consoles are monitored by the Security Team and unusual activity noted is researched and resolved.

The organization periodically assesses the sufficiency of its information systems to capture and report data that are timely, current, accurate, and accessible.



For high severity incidents, Root Cause Analysis (RCA) is performed through various tools and meetings in order to improve the quality of the solution RavenDB provide to customers.

SLA with third parties exist and include monitoring the process and the access.

Management assesses the risks associated with subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner.

CC5.0 Control Activities

Internal Audit

RavenDB Ltd. established internal audit procedures and techniques as part of the company Risk Management implementation.

Each department manager is required to hold an internal audit for the processes and procedures in his field at least once a year. Audit procedures steps are:

- (1) Assess current processes and procedures.
- (2) Analyze and compare results against internal control objectives to determine whether audit results comply with internal policies and procedures as well as federal and state rules and regulations.

CC6.0 Logical and Physical Access Controls

Logical Access Management

Logical Security – RavenDB Personnel Access:

Employees get access to company systems on a need-to-know basis. Access is guarded by the Access Control Policy and Role Based Access Control Matrix.

Logical Security – Customer Access:

RavenDB offers:

- login via email with an optional 2FA
- authentication using RavenDB license key

Physical and Environmental Security:

Visitors to RavenDB Ltd. are required to call their host in order to enter the offices. Visitors will be escorted during their visit by an employee, all in accordance with ISP-07 Physical and Environmental security procedure policy.

RavenDB Ltd. has outsourced hosting of RavenDB servers, including the physical and environmental security of facilities housing such servers, to AWS.

RavenDB Ltd. restricts access to its customer data and sensitive internal systems using multiple approaches:



- Workstations and servers' protection:
 - (1) Central solution to remotely manage and monitor suspected malicious activity of computers, with the ability to initiate remediation process
 - (2) Central solution to detect suspicious users activity
 - (3) Network firewall - for intrusion prevention
 - (4) WIFI secured with WPA2 standard
 - (5) VPN to securely connect to the office digital resources from outside of the physical perimeter
 - (6) User passwords should be set to auto-expire every 180 days and should force users to use strong passwords. User accounts, passwords, and keys provided remain confidential and not shared between employees.
- Logical access restrictions: new user creation and permissions modifications are restricted and carried out by the IT team after being approved by the relevant Project manager, and under the supervision of the Information Security manager. Complete access for a specific employee is calculated as the combined access based on all groups the employee is part of.

Remote Access

Remote systems are accessed using VPN software allowing for encrypted connection using 2 factor authentication.

CC7.0 System Operations

Penetration Test

RavenDB Ltd. performs Penetration Test on an annual basis. It is performed by a 3rd party IT security company. Tests report is reviewed by CISO and CTO and remediations are planned according to the severity of the findings.

Incident Management

RavenDB Incident Management procedure addresses the means necessary to ensure effective response to incidents relevant to the system, identifying the lifecycle of the incident management, including the incident identification, investigation, prioritization and mitigation.

Based on ISP-10 Information security incident response and breach notification procedure:

The company has established an Incident Response Team (IRT) dedicated to managing security-related incidents in a quick, effective, and organized manner. This team is authorized to take all necessary actions to contain, mitigate, and resolve any security incidents that may arise. The IRT is responsible for promptly investigating suspected intrusions or other security incidents and reporting its findings to management in a timely and cost-effective manner. The size and



composition of the IRT are flexible, adjusting based on the specific skills required to handle each unique incident, and may include external consultants or suppliers as needed.

The IRT is tasked with overseeing both the response and recovery phases of incident management, remaining active until the incident is fully resolved. The incident response process consists of several key stages: preparation, detection and analysis, eradication and recovery, and post-incident activities. During the preparation phase, the IRT focuses on preventive measures such as risk assessments, network security, and user training to minimize the likelihood of incidents. In the detection and analysis phase, the team identifies and assesses potential security breaches, using both automated tools and manual processes.

When an incident is confirmed, the IRT takes immediate steps to contain the threat, limit damage, and, if possible, identify the source of the attack. The team also meticulously documents every action taken, collecting evidence in accordance with legal standards to ensure admissibility in court if necessary. In the eradication and recovery phase, the IRT works to remove any malicious components, restore normal system operations, and implement measures to prevent future incidents.

Finally, post-incident activities include a "lessons learned" meeting to review the incident, assess the response, and identify areas for improvement. The Chief Information Security Officer (CISO) is responsible for documenting the incident, tracking corrective actions, and updating company management on the status of these actions. Additionally, the IRT, in consultation with legal advisors, ensures that all regulatory and contractual breach notification requirements are met, with the CEO overseeing communications with regulatory authorities.

Antivirus

The company's network and employee computers store sensitive information, such as customer data, source code, and personal information, making it essential to implement robust security measures. This procedure outlines the necessary network and computer security controls that employees must follow to protect these valuable information assets.

As part of the security measures, managed antivirus software will be installed on all company computers. This software allows centralized control over antivirus settings, ensuring consistent protection across all devices. The antivirus will automatically update virus signatures whenever the computer is connected to the internet, ensuring the system remains up to date against new threats. To maintain security, the software will be configured to prevent users from disabling it or changing its settings.

The IT department is tasked with monitoring antivirus alert logs and addressing any security issues or non-conformances that may arise, ensuring ongoing protection of the company's sensitive information.



Availability Procedures

Production Monitoring

Production systems are continuously monitored using a comprehensive suite of tools to ensure optimal performance, security, and reliability. The primary monitoring platform is Zabbix server software, which provides detailed insights into system health and performance metrics across the infrastructure. Additionally, AWS services such as GuardDuty, Inspector, and CloudTrail are integrated to enhance security monitoring, with GuardDuty detecting threats, Inspector assessing vulnerabilities, and CloudTrail providing detailed logs of account activity. For log aggregation and real-time alerting, Grafana is employed, offering a centralized view of system logs and enabling teams to quickly identify and respond to potential issues.

All alerts generated by these monitoring tools are systematically logged and routed to the appropriate channels for swift action. Alerts are sent to designated Slack monitoring channels, ensuring that team members are immediately notified of any anomalies or critical events. Furthermore, alerts are also distributed via email to specific aliases corresponding to the teams responsible for the affected systems, ensuring that the right personnel are informed and can take timely action to mitigate any issues. This multi-faceted monitoring approach helps maintain the stability and security of production systems, allowing teams to proactively address potential problems before they escalate.

Database Backup

Databases are managed on a highly reliable RavenDB Production Cluster, ensuring optimal performance and data availability. To safeguard the data, a comprehensive backup strategy is in place. Full database backups are executed every 10 days, capturing a complete snapshot of the data. In addition to this, incremental backups are performed every hour, which record any changes made since the last backup. This frequent backup process ensures minimal data loss in the event of any unexpected issues. All backup files are securely stored on cloud storage, with robust encryption applied to ensure data is protected at rest, maintaining the highest standards of security and compliance.

Restoration

In the event of a failure, databases can be restored from backups stored in secure cloud storage, ensuring minimal data loss. Virtual machines can be redeployed quickly using volume snapshots, which capture their exact state at specific points in time. This approach enables rapid recovery and helps maintain business continuity with minimal disruption.



Disaster Recovery Plan (DRP)

The company will establish a Business Continuity Plan (BCP) team that includes both technical and management staff, as outlined in ISP-16. This team is tasked with ensuring the company's preparedness for any disruptions by developing procedures, implementing technical measures, and conducting periodic tests and evaluations. In the event of an emergency, the BCP team is responsible for executing the business continuity plan swiftly and effectively to minimize downtime and maintain operations.

The CEO holds the responsibility for formally announcing the activation of the business continuity procedures when necessary. The BCP team leader plays a crucial role in coordinating all efforts within the team, ensuring seamless communication, and reporting directly to company management. Additionally, the team leader is responsible for documenting all actions and decisions in a detailed log file to maintain a clear record of the process.

To ensure the effectiveness of the BCP, the Chief Information Security Officer (CISO) is responsible for developing an annual test plan that covers all scenarios outlined in the procedure. After each test, the BCP team conducts a "lessons learned" meeting to review performance and identify areas for improvement. The CISO prepares a summary of the test results, which is then shared with company management and the BCP team. The CISO also tracks and follows up on any corrective actions identified during the testing process, ensuring continuous improvement of the company's business continuity readiness.

CC8.0 Change Management

Details can be found in the following policies:

ISP-11 Change management procedure policy describing the change management when it comes to company IT infrastructure. The company policy requires that significant changes to IT infrastructure, including new services or architectural updates, undergo a thorough review and authorization process involving the CEO, CTO, and CISO before implementation. The CTO is responsible for ensuring these changes comply with all requirements and are properly documented in Youtrack. For non-significant changes with potential security impacts, approval from the CISO is necessary, and these changes are recorded in Youtrack's "security approval" section with minimal documentation. This process ensures that all changes are controlled, security risks are managed, and system integrity is maintained.

CC9.0 Risk Mitigation

Backup and Restoration

In the event of a failure, databases can be restored from backups stored in secure cloud storage, ensuring minimal data loss. Virtual machines can be redeployed quickly using volume snapshots, which capture their exact state at specific points in time. This approach enables rapid recovery and helps maintain business continuity with minimal disruption.

Vendor risk management

RavenDB Ltd. maintains a list of approved vendors (suppliers). To be approved, each new vendor needs to undergo an evaluation process during which RavenDB Ltd.:

- assess the sensitivity of data processed by the vendor.
- assess the characteristics of data processed by the vendor.
- analyze compliance level and security of the vendor.
- contact the vendor if required to obtain additional information and documentation.
- consult questionable points with lawyer and company management.

Confidentiality Procedures

RavenDB takes reasonable steps to ensure that access to personal data is limited to a need to know and/or need to access basis and that all employees receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access to and use of Controller Personal Data.

Attachment B

Attachment B

Principal Service Commitments and System Requirements

- RavenDB's security commitments regarding the systems and operations are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided to user entities. Those objectives are based on the service commitments that the service organization makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that service organization has established for the services.
- Security commitments are standardized and include, but are not limited to, the following:
 - Security principles within the fundamental designs of the RavenDB system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
 - Use of encryption technologies to protect customer data both at rest and in transit.
 - Use strong identity management processes to secure data and systems from intrusion.
 - Manage infiltration, intrusions, insider threats and anomalies by understanding who is on our networks, for what reasons, and what data is accessible.
- The service organization establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated in RavenDB's systems policies and procedures, system design documentations, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how systems are operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of relevant services provided to its customers.